자기장을 이용한 무선 은닉채널 시스템 개발

전용성, 이상우, 정지혁*, 최형준*
한국전자통신연구원, *고려대학교

ysjeon@etri.re.kr, ttomlee@etri.re.kr, *graycat@korea.ac.kr, *tiger8135@korea.ac.kr

Development of wireless covert channel system using magnetic fields

YongSung Jeon, SangWoo Lee, JiHyuk Jung*, HyeongJun Choi*
Electronics and Telecommunications Research Institute, *Korea Univ.

요 약

본 논문은 cpu 부하 증가에 의해 발생하는 자기장을 이용한 무선 은닉채널 시스템 개발을 소개한다. 본 논문에서 제안하는 변조 방법인 MTGM(Modified Time-Gap Modulation)은 자지장 신호의 발생 시간을 환경에 따라 가변할 수 있는 장점을 가진다. 시험을 통해 확인한 은닉채널의 수신 성공률은 40%에서 100%사이로, 환경에 따라서 성공률의 변동이 크지만, 통신 채널로서의 최소한의 안정성을 보장하고 있음을 알 수 있다.

Ⅰ. 서 론

은닉 채널은 비정상적인 통신 채널을 생성하여 통신 권한이 없는 악의적인 개체에게 정보를 전달하는 공격 유형이다. 또한, 은닉 채널은 적법한 의사소통에서 사람들이 다른 사람에게 들키지 않고 의사 소통할 수 있도록 보장하는 숨겨진 의사소통 방법으로 정의될 수 있다[1].

자기장을 이용한 은닉채널과 관련한 기존 논문은 대표적인 것으로 3 가지가 존재하며, 이들 논문의 특징점들을 표 1 에 정리하였다. 기존논문 1 은 컴퓨터의 입출력을 수행하는 동안 발생한 자기장 변화를 스마트폰에서 수신할 수 있으며, 이를 은닉채널에 이용할 수 있음을 보여주었다. 앞서 말한 자기장의 생성은 하드디스크나 전류 변화에 의한 자기장 발생 원리를 이용하며, 수신은 스마트폰에 내장된 자기장센서를 이용한다. 기존논문 2 는 Faraday shielding 이 되어 있는 벽을 통해 은닉채널을 구축할 수 있는가에 대한 내용이다. 기존논문 3 은 자기장생성으로는 CPU core 를 이용하였으며, 수신에는 스마트폰의 자기장센서를 이용하였다. 이 논문은 수신 스마트폰을 송신 컴퓨터에서 생성하는 자기장 발생 영역에 놓고 정보를 송수신할 수 있는가에 대한 실험을 진행하였다.

표 1. 자기장을 이용한 은닉채널 개발 기존 논문[2,3,4]

기존논문	은닉채널 형성 방식	수신 장치	최대 bit rate	최대 거리
논문 1 – Hard Disk Drive	Hard Disk Drive (magnetic)	smartphone	2 bps	0~12 cm (laptops)
논문 2-ODINI	CPU cores	Magnetic sensor	40 bps	100 ~ 150cm
논문 3-MAGNETO	CPU cores	smartphone	5 bps	0~12 cm (desktops)

본논문에서는 기존논문 3 과 유사한 cpu 부하증가에 의해 발생하는 자기장을 이용하고, 자기장의 수신장치로 스마트폰을 이용하는 은닉채널 시스템 개발 내용을 소개한다.

Ⅱ. 본론

본논문에서는 cpu 부하증가에 의해 발생하는 자기장을 이용한 무선 은닉채널의 송신 패킷 구조를 그림 1 과 같이 제안한다.

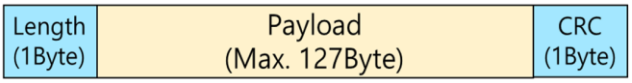

그림 1. 제안하는 자기장 은닉채널 패킷 구조

또한, 본논문에서는 자기장을 이용한 은닉채널의 변조 방식으로 그림 2 와 같은 방법을 제안한다. 제안된 은닉채널 변조방법은 일정시간 자기장 신호를 발생시킨 후 다음 자기장을 발생시키는 시간의 간격, 즉 Time-Gap 을 이용한다. 따라서 본 연구에서 설계된 변조 방법을 MTGM(Modified Time-Gap Modulation)이라고 명명한다.

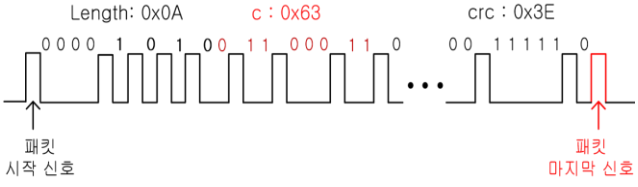

그림 2. 제안하는 자기장 은닉채널 변조 방법

MTGM 은 그림 2 에서 보는 바와 같이, 자기장 신호와 다음 자기장 신호사이의 시간이 bit 의 개수를 결정하게 된다. 그리고, 패킷의 시작 bit 값은 '0'으로 정의하고, 자기장 신호가 수신되지 않는 동안은 계속 동일한 bit 값을 유지하다가, 다음 자가장 신호가 수신되면 bit 값은 반전되는 것으로 정의한다.

MTGM 이 다른 변조 방법에 비해 유리한 이유는 자기장 신호가 발생하는 시간(이하 "신호 시간"으로 칭함)은 정보 값을 가지지 않는 것이다. 따라서, 시스템의 특성 또는 주변의 환경에 맞추어 "신호 시간"을 변경하여도 전달되는 정보 bit 값에는 아무런 영향을 미치지 않는다. 반면, 실제 정보 값들은 자기장 신호 사이의 시간 즉, 자기장 신호가 없는 구간의 시간에 의해 결정된다. 따라서, 한개의 bit 시간(이하 "bit 시간"으로 칭함)은 송신장치와 수신장치 사이에 미리 공유되어야 한다. 본 논문의 자기장 은닉채널 시스템에서는 "bit 시간"을 500ms 로 설정하고, "신호시간"은 어느정도 가변하여도 자기장 송수신은 정상적으로 이루어짐을 확인하였다.

그림 3. 자지장 은닉채널 시스템

본 논문에서 제시하는 자기장 은닉채널 시스템은 그림 3 과 같다. 데스크탑 컴퓨터를 은닉채널 송신 장치로 사용하고 스마트폰을 수신 장치로 사용한다. 송신 장치의 데스크탑 PC 의 OS 로는 "Ubuntu 20.04.3 LTS"를 사용하였고, 수신 장치는 Galaxy S22 에서 Android 13 를 사용하여 수신용 앱을 자체 제작하였다.

표 2. 시험에 사용된 페이로드들

페이로드 번호	페이로드 내용	페이로드 길이
1	covert1	7
2	covert22	8
3	covert333	9
4	covert4444	10
5	covert55555	11
6	covert666666	12
7	covert777777	13
8	covert8888888	14
9	covert99999999	15
10	covert0000000000	16

개발된 자기장 은닉채널 시스템의 기능을 시험하기 위하여 표 2 와 같은 페이로드들을 사용하였다. 이들 페이로드들은 그림 1 의 은닉채널 패킷 구조에서 페이로드 부분에 위치하게 된다. 그림 4 는 페이로드 내용이 "covert1"에 대한 수신 파형을 나타내고 있다. 그림에서 빨간색 수직선은 자기장 파형의 시작점을 나타내고, 노란색 수평선은 bit 값 '0' 또는 '1'을 구분하는 Threshold 값을 나타낸다. 여러차례 시험을 수행한 결과, 표 2 에 나타낸 10 개의 페이로드에 대해 수신 성공률이 40%에서 100%사이가 되었다. 자지장의 특성 상, 시험 환경에 따라 자기장의 송-수신 기능이 민감하게 동작하는 것으로 판단된다.

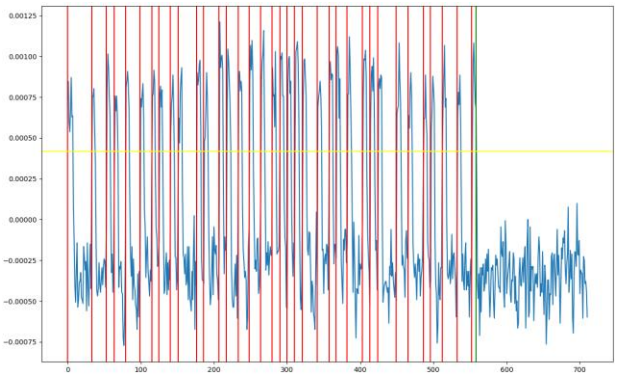

그림 4. "covert1" 페이로드에 대한 자기장 수신 파형

Ⅲ. 결론

본논문에서는 cpu 부하증가에 의해 발생하는 자기장을 이용한 무선 은닉채널 시스템을 개발하였다. 개발된 시스템의 성능을 평가해본 결과, 10 개의 페이로드에 대해, 수신 성공률이 40%에서 100%사이가 되었다. 환경에 따라 성공률의 변동이 크지만, 통신 채널로서의 최소한의 안정성을 보장하고 있음을 알 수 있다.

.

ACKNOWLEDGMENT

이 논문은 2024 년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2020-0-00913, 무선 은닉채널 위험성 검증 연구)

참 고 문 헌

[1] B. W. Lampson, A note on the confinement problem,Commun. ACM, vol. 16, no. 10, pp. 613- 615, 1973.

[2] N. Matyunin, J. Szefer, S. Biedermann, and S. Katzenbeisser, "Covert channels using mobile device's magnetic field sensors," in Design Automation Conference (ASP-DAC), 2016 21st Asia and South Pacific, 2016, pp. 525- 532.

[3] Y. E. Boris Zadov Andrey Daidakulov Mordechai Guri, "ODINI: Escaping Sensitive Data from Faraday-Caged, Air-Gapped Computers via Magnetic Fields," 2018.

[4] Mordechai Guri, Andrey Daidakulov, Yuval Elovici, "MAGNETO: Covert Channel between Air-Gapped Systems and Nearby Smartphones via CPU-Generated Magnetic Fields," in Future Generation Computer Systems vol. 115, 2021. Feb., pp115- 125.